

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-274999

(43)Date of publication of application : 08.10.1999

(51)Int.Cl.

H04B 7/26

G07B 15/00

G07B 15/00

H04L 9/08

(21)Application number : 10-076909

(71)Applicant : HITACHI LTD
HITACHI INF & CONTROL SYST LTD

(22)Date of filing : 25.03.1998

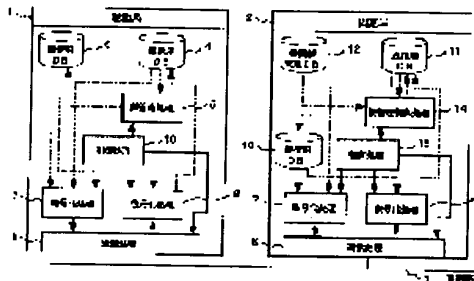
(72)Inventor : NOZATO MASAYA
KAYUKAWA SATORU
IINO TAKAYUKI
ORIMO MASAYUKI
FUKUZAWA YASUKO
ISHIDA SHUICHI

(54) MOBILE COMMUNICATION METHOD AND MOBILE COMMUNICATION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a mobile communication system where the start of communication between a mobile station and a stationary station is quickened and a key in use is quickly and securely switched against an illegal use of an encryption key or the like.

SOLUTION: Common keys with plural versions are available for encryption communication between a stationary station and plural mobile stations, each mobile station 1 manages a sole key version and its symmetrical key (ordinary key and emergency key) in a form of key information DB 6, and the stationary station 2 manages plural key versions and their symmetrical keys in a way of key information management DB 12. The mobile station 1 sends a key version of its own station on a communication request, the stationary station 2 discriminates whether or nor a usual key of the received key version is effectively supported and replies the version and the key application (normal), when it is effectively supported. When the usual key is invalid, the stationary station 2 replies the version and the key application (urgent). The mobile station 1 discriminates the key version and the key application replied from the stationary station 2 and switches the key used by its own station into the urgent key, even if the key version is the same when the key application is the 'urgent key'.



LEGAL STATUS

[Date of request for examination] 09.08.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3445490

[Date of registration] 27.06.2003

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of

rejection]

[Date of extinction of right]

* NOTICES *

JPO and NCIPi are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1] In the mobile correspondence procedure whose common use of two or more versions of said key enables the share of the key (cryptographic key) used for encryption or a decryption of the bidirectional cryptocommunication of a fixed station and a mobile station with two or more mobile stations, and is enabled While a mobile station transmits the version of the usable cryptographic key of a local station to the communication link demand to a fixed station Check that this version is contained in a response from a fixed station, and, as for a fixed station, the receiving version from a mobile station confirms whether it is contained in the key information which a local station manages. It is the mobile correspondence procedure characterized by matching and managing the identifier and its key used of the mobile station concerned during a communication link while answering the mobile station which determined the version concerned as the key used and sent said communication link demand, when contained.

[Claim 2] It is the mobile correspondence procedure which a fixed station answers a mobile station in claim 1 in the version of the one or the dummy of key information effective when the receiving version from a mobile station is not contained in the key information which a local station manages, and is characterized by the mobile station concerned broadcasting the communication link demand by it again when the response version from a fixed station is usable at a local station.

[Claim 3] In the mobile correspondence procedure whose common use of two or more versions of said cryptographic key enables the share of the cryptographic key used for encryption or a decryption of the bidirectional cryptocommunication of a fixed station and a mobile station with two or more mobile stations, and is enabled Each mobile station and a fixed station the cryptographic key of the usable version of a local station, respectively Usually, while it manages with the key (they are usually a key and an alternative key) of the pair corresponding to the key application business and for an alternative and a mobile station transmits the version of the usable cryptographic key of a local station to the communication link demand to a fixed station When the version and key application which are included in a response from a fixed station are checked, the version of a response is the same as that of a local station and a key application is usually business It is confirmed whether the cryptographic key used for the communication link of a local station is included in said two or more versions to which a local station manages [the receiving version from a mobile station] a fixed station by usually considering as as [key]. While effective/invalid of said usual key are checked, and usually determining a key as the key used and answering the mobile station concerned which sent said communication link demand in a version and a key application (usually business) concerned when effective when contained The mobile correspondence procedure characterized by matching and managing the identifier and its key used of the mobile station concerned during a communication link.

[Claim 4] As for a fixed station, the receiving version from a mobile station is contained in the version which a local station manages in claim 3. And when [said] a key is usually an invalid By determining a key and the alternative key which makes a pair concerned as the key used, while answering the mobile station which sent said communication link demand in a version and a key application (for an alternative) concerned, usually It is the mobile correspondence procedure characterized by matching and managing the identifier and its key used of the mobile station concerned during a communication link, for the mobile station concerned making the usual key of a local station an invalid from a fixed station when the key application of a response is an object for an alternative, and using as the key used of the cryptocommunication of a local station the alternative key which makes it and a pair.

[Claim 5] In the mobile correspondence procedure whose common use of two or more versions of said cryptographic key enables the share of the cryptographic key used for encryption or a decryption of the bidirectional cryptocommunication of a fixed station and a mobile station with two or more mobile stations, and is enabled Each mobile station and a fixed station the cryptographic key of the usable version of a local station, respectively Usually, while it manages with the key (they are usually a key and an alternative key) of the pair corresponding to the key application business and for an alternative and a mobile station transmits the version and key application (usual or alternative) of an usable cryptographic key of a local station to the communication link demand to a fixed station The version contained in a response from a fixed station is checked. When the version of a response is the same as that of a local station Use the cryptographic key of a key application which transmitted from the local station, and when the version which received from the mobile station is contained in two or more versions which a local station manages, a fixed station If the received key application is usual, usually check effective/invalid of a key, and when effective, while answering the mobile station which sent said communication link

demand, said version which said alternative key was determined as the key used in the case of the invalid, and usually received the key. The mobile correspondence procedure characterized by matching and managing the identifier and its key used of the mobile station concerned during a communication link.

[Claim 6] It is the mobile correspondence procedure characterized by the thing [usually repealing a key] concerned in claims 3, 4, or 5 when the key application modification directions of said version as which management of effective/invalid of a key was usually specified from high order equipment in a fixed station are received.

[Claim 7] It has the fixed station which has a communications processing means and encryption / decryption processing means, and two or more mobile stations which are carried on a mobile and have a communications processing means and encryption / decryption processing means. In the mobile communication system whose common use of two or more versions of said cryptographic key enables the share of the cryptographic key used for the bidirectional cryptocommunication of a mobile station and a fixed station with two or more mobile stations, and is enabled a mobile station. While transmitting the key version of a local station to the key version used for the communication link of a local station, the key information database which stores the key information containing a key, and the communication link demand to a fixed station. A key management processing means to manage the key used of a local station in contrast with the key version contained in a response from a fixed station is established. A fixed station. Two or more key versions used for the communication link with a mobile station, and the key information management database which stores the key information containing the key. When the key version which received from the mobile station is contained in said key information management database, the key of the key version concerned is determined as the key used. Mobile communication system characterized by forming the communication link key information database which matches and manages a key supervisory control processing means to answer a mobile station in the key version concerned, and the identifier and its key used of a mobile station under communication link.

[Claim 8] In claim 7, a fixed station and a mobile station usually contain the key application of a /alternative, the usual key of a corresponding pair, and an alternative key for every key version as said key information. To a fixed station. It has the function manager which makes an invalid use of the usual key of an applicable key version with the key application modification directions from a high order. Said key supervisory control processing means of a fixed station. When the usual key of the key version which received from the mobile station is an invalid, determine a pair of alternative key as the key used, and a mobile station is answered in the key version and key application (alternative). Said key management processing means of a mobile station is mobile communication system characterized by making the usual key of a key information database into an invalid from a fixed station when the key application of a response is an object for an alternative.

[Claim 9] In claim 7, a mobile station usually contains the key application of a /alternative, the usual key of a corresponding pair, and an alternative key for every key version as said key information. A fixed station contains the usual key which serves as the usual key application for every key version as said key information. And while the key version and key application by key application modification directions receive and manage a substitute alternative key from a high order, it has the function manager concerned which usually makes use of a key an invalid. When the usual key of the key version which received from the mobile station is an invalid, said key supervisory control processing means of a fixed station determines said alternative key as the key used, and answers a mobile station in the key version and key application (alternative). Said key management processing means of a mobile station is mobile communication system characterized by making the usual key of a key information database into an invalid from a fixed station when the key application of a response is an object for an alternative.

[Claim 10] Said mobile station is the communication device with which said mobile communication system is an electronic toll collection system of a turnpike, and said fixed station is prepared in a tollgate or a road side in claims 7, 8, or 9, and mobile communication system constituted by the communication device carried in the car using a turnpike.

[Translation done.]

* NOTICES *

JPO and NCIP are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] Especially this invention relates to the mobile communication which manages a cryptographic key to an alteration-proof secretly between a fixed station and a mobile station about the cryptocommunication approach.

[0002]

[Description of the Prior Art] The spread of the mobile communication by the cellular phone or the land mobile radiotelephone is remarkable, and utilization of the electronic toll collection system (ETC) of a turnpike etc. is also in nearness. The electronic toll collection system of a turnpike is a system which **** a tariff using radio between the point-to-point-communication means (fixed station) installed in the tollgate road side, and the migration means of communications (mobile station) carried in the car which runs a turnpike. In the accounting of ETC, since information about individual privacy, such as a user's authentication, deposit information, etc., is transmitted and received on radio, in order to prevent leakage of these information, and an alteration, reservation of the security which used cryptocommunication becomes indispensable.

[0003] The key information for enciphering a plaintext and decrypting a cipher for prevention of the nondisclosure of the contents of a communication link or an alteration, is used, for example, like a publication on "the Internet security" foundation and a cure technique (work besides Ryoichi Sasaki, Ohm-Sha, pp 95-102)" The "key encryption key" called KEK (Key Encrypting Key) is beforehand set up between a transmitting person and an addressee. A transmitting person enciphers the "data encryption key" called DEK (Data Encrypting Key) which enciphers data using this KEK, and transmits to an addressee, and an addressee decrypts DEK using KEK and is decoding the cipher using DEK.

[0004] Moreover, a transmitting person receives an addressee's public key, sends DEK which enciphered this public key as KEK to an addressee, and also has a method of sharing DEK between a transmitting person and an addressee. Management of these encryption key has an approach by the card, and there are also deterioration of key information and risk of loss. Generally, it has managed for every mobile station by the key server.

[0005] The procedure of the cryptocommunication of the mobile station which uses a key server for drawing 11, and a fixed station is shown. The key server has managed the key K1 of a mobile station A, the key K2 of a mobile station B, and the key of a total displacement station on the key managed table. When the mobile station A holding a key K1 communicates with a fixed station, the communication link demand by the identifier of the ** mobile station A is published. ** In a fixed station, answer a key server in the key of a mobile station A, and an inquiry and ** key server answer a fixed station in the key K1 of a mobile station A. ** A fixed station performs cryptocommunication to a mobile station A using a key K1 (or key K11 which generated data K1 as the species), and the ** mobile station A decodes a cipher using a key K1 (or key K11 decoded from data K1), and communicates with a fixed station by the cipher using a key K1 (or key K11).

[0006] In addition, key information is upgraded periodical or if needed, in order to prevent the unauthorized use by leakage (tapping and decode). The key information which a key server manages is a key common to the key or mobile station of a proper to a mobile station, and, in the case of the latter, a key version in use for every mobile station is managed. That is, proper information or version information is sufficient as the keys K1 and K2 illustrated to drawing 9.

[0007]

[Problem(s) to be Solved by the Invention] As mentioned above, since time amount is taken by the communication link initiation between a mobile station and a fixed station since a fixed station carries out the inquiry of the key used at every communication link demand from a mobile station to a server, and the key information on KEK or DEK is directly transmitted to a fixed station from a server by the method which manages the key information on cryptocommunication by the key server, the risk of leakage is also high.

[0008] Especially, in ETC, in order to prevent the interference of a wireless electric wave used for tariff ****, it is necessary to set up a communication region narrowly. On the other hand, since the car which performs an electronic fee collection system serves as employment which passes a tollgate, without stopping, the time amount in which the communication link between a fixed station and a mobile station is possible is very short. For example, when a car runs a 4m communication region at the high speed of 180 km/h, the time amount which can communicate is only 80ms. Since the high-speed response between a car and a tollgate is difficult and tariff **** by high-speed passage becomes impossible, it stops therefore, being useful to a delay dissolution in a tollgate by the

key management method by the server.

[0009] However, a fixed station is unable to manage the key information on many and unspecified mobile stations instead of a server in a Prior art. Since each mobile station does not understand whether it advances to which tollgates all over the country, and a communication link is started, each fixed station is because management of the key information on a total displacement station is needed. Even when a mobile station uses a common key, since the key version of a mobile station is updated at the time of each automobile inspection etc., it is necessary to apply possible [common use of two or more key versions], and management of a fixed station becomes difficult.

[0010] Moreover, when an unauthorized use is revealed in a key version in use, even if it can do the immediate steps to a mobile station with damage, they cannot respond immediately to many other mobile stations which are using the key version, but have a possibility that damage may be expanded.

[0011] The purpose of this invention is to offer the migration correspondence procedure which the trouble of mobile communication including the conventional cipher can be conquered, and the risk of leakage of key information can start a communication link by high response few, or can perform renewal of a key in emergency easily.

[0012] Moreover, it is in offering the unnecessary simple migration communication system of high security of a key server. Furthermore, it is in offering the electronic toll collection system of the turnpike as for which tariff collection (accounting) is made for a short time (under high-speed passage) certainly.

[0013]

[Means for Solving the Problem] This invention for attaining the above-mentioned purpose enables the share of the key (cryptographic key) used for encryption or a decryption of the bidirectional cryptocommunication of a fixed station and a mobile station with two or more mobile stations. And in the mobile correspondence procedure whose common use of two or more versions of said cryptographic key is enabled, while a mobile station transmits the version of the usable cryptographic key of a local station to the communication link demand to a fixed station Check that this version is contained in a response from a fixed station, and, as for a fixed station, the receiving version from a mobile station confirms whether it is contained in the key information which a local station manages. When contained, while answering the mobile station which determined the version concerned as the key used and sent said communication link demand, it is characterized by matching and managing the identifier and its key used of the mobile station concerned during a communication link.

[0014] The above-mentioned fixed station answers a mobile station in the version of the one or the dummy of key information, when the receiving version from a mobile station is not contained in the key information which a local station manages, and when the mobile station concerned has an usable response version from a fixed station at a local station, it is characterized by broadcasting a communication link demand again by using the version of this response as the key used. Consequently, by the fixed station, the version of resending is accepted in the key used and managed during a communication link.

[0015] Since according to this invention a fixed station can share two or more key versions of a common key without derangement among two or more mobile stations and the key used can be determined for fixed-station itself, a communication link can be started immediately.

[0016] Each mobile station and a fixed station this invention moreover, the cryptographic key of the usable version of a local station, respectively Usually, while it manages with the key (they are usually a key and an alternative key) of the pair corresponding to the key application business and for an alternative and a mobile station transmits the version of the usable cryptographic key of a local station to the communication link demand to a fixed station When the version and key application which are included in a response from a fixed station are checked, the version of a response is the same as that of a local station and a key application is usually business It is confirmed whether the cryptographic key used for the communication link of a local station is included in said two or more versions to which a local station manages [the receiving version from a mobile station] a fixed station by usually considering as as [key]. While effective/invalid of said usual key are checked, and usually determining a key as the key used and answering the mobile station concerned which sent said communication link demand in a version and a key application (usually business) concerned when effective when contained It is characterized by matching and managing the identifier and its key used of the mobile station concerned during a communication link.

[0017] As for the above-mentioned fixed station, the receiving version from a mobile station is contained in the version which a local station manages. Moreover, when [said] a key is usually an invalid, [and] By determining a key and the alternative key which makes a pair concerned as the key used, while answering the mobile station which sent said communication link demand in a version and a key application (for an alternative) concerned, usually It is characterized by matching and managing the identifier and its key used of the mobile station concerned during a communication link, for the mobile station concerned making the usual key of a local station an invalid from a fixed station, when the key application of a response is an object for an alternative, and using as the key used of the cryptocommunication of a local station the alternative key which makes it and a pair.

[0018] Furthermore, when said key application modification directions of a version in the above-mentioned fixed station with which management of effective/invalid of a key was usually specified from high order equipment are received, it is characterized by the thing [usually repealing a key] concerned.

[0019] Since according to this invention on-line processing of the change in the alternative lock which makes the usual key of a key version an invalid and each mobile station holds can be carried out under communication link, without transmitting a cryptographic key when an unauthorized use is revealed, urgent correspondence can perform to high security. In addition, below, the method by the pair of a key and an alternative key (an example urgent key) is usually called a symmetry key cipher system.

[0020] In addition, the version and key application of a key which are used for a communication link demand by the local station from a mobile station above are transmitted, and only the version which opted for use by the fixed station may be made to answer. According to this, key decision processing of a fixed station is simplified further.

[0021] The mobile communication system of this invention which applies the above-mentioned mobile correspondence procedure It has a fixed station and two or more mobile stations carried on a mobile. A mobile station While transmitting the key version of a local station to the key version used for the communication link of a local station, the key information database which stores the key information containing a key, and the communication link demand to a fixed station A key management processing means to manage the key used of a local station in contrast with the key version contained in a response from a fixed station is established. A fixed station Two or more key versions used for the communication link with a mobile station, and the key information management database which stores the key information containing the key, When the key version which received from the mobile station is contained in said database, the key of this key version is determined as the key used. It is characterized by forming the communication link key information database which matches and manages a key supervisory control processing means to answer a mobile station in the key version concerned, and the identifier and its key used of a mobile station under communication link.

[0022] A fixed station and a mobile station usually contain the key application of a /alternative, the usual key of a corresponding pair, and an alternative key for every key version as said key information. Moreover, to a fixed station It has the function manager which makes an invalid use of the usual key of an applicable key version with the key application modification directions from a high order. Said key supervisory control processing means of a fixed station When the usual key of the key version which received from the mobile station is an invalid, determine a pair of alternative key as the key used, and a mobile station is answered in the key version and key application (alternative). It is characterized by said key management processing means of a mobile station making the usual key of a key information database an invalid from a fixed station, when the key application of a response is an object for an alternative.

[0023] Or a fixed station is characterized by coming to have the function manager concerned which usually makes use of a key an invalid, while the according [usually including only a key] to the key application modification directions from high order key version which serves as the usual key application for every key version as said key information, and a key application receive a substitute alternative key and managing.

[0024] The example of 1 application of the above-mentioned mobile communication system is the electronic toll collection system (ETC) of a turnpike, and the communication device with which a fixed station is prepared in a tollgate or a road side, and a mobile station are constituted as a communication device carried in the car using a turnpike.

[0025] High security is securable while a system configuration simplifies, since the mobile communication system of this invention makes a key server unnecessary. Moreover, since the high-speed processing of the communication link between a fixed station and a mobile station can be carried out, the processing time of ETC of a turnpike is shortened and tariff **** in high-speed passage becomes possible.

[0026]

[Embodiment of the Invention] Hereafter, the migration correspondence procedure by 1 operation gestalt of this invention and its system are explained to a detail, referring to a drawing. In addition, the same sign is given to the equivalent component through each drawing.

[0027] The configuration of the outline of the electronic toll collection system of the turnpike which applies this invention to drawing 10 is shown. The fixed station 100 of ETC arranged in the tollgate enciphers and carries out the radio traffic of the confidential information through the antenna 110 installed in the upper part or the flank of the lane 200 only for automatic tariffs between the mobile stations 310 which the car 300 which advanced into the communications area 210 shown with a broken line carries, carries out automatic collection of the tariff, and reports it to high order equipment.

[0028] Extension of the communications area 210 which an antenna 110 covers is at most several m, in order to prevent interference with other vehicle. For this reason, communication must be ended in the mobile station 310 of the car passed at high speed, and about 0.1 seconds or less, and a high-speed response is needed for the cryptocommunication between a fixed station 100 and a mobile station 310.

[0029] Drawing 1 is the block diagram of the migration communication system by one example of this invention. It consists of a communication device (mobile station) 1 carried in the mobile, a communication device (fixed station) 2 installed in the road side which communicates with a mobile station 1, and a channel 3 which contracts a mobile station 1 and a fixed station 2. Although a channel 3 does not ask wireless and a cable, it is based on the wireless through an antenna by this example. Below, although the cryptocommunication between a mobile station 1 and a fixed station 2 is explained, also when enciphering only confidential information and combining with a plaintext, it contains. Moreover, although the key for encryption/decryption points out above-mentioned "a data encryption key (DEK)", "a key encryption key (KEK)" may be used.

[0030] The decision of the key which a mobile station 1 reads the key related information from the fixed station 2 accumulated in DB4 for a communication link which is storing the transmit information, receipt information, and key related information (a key is not included) of a plaintext, and DB4 for a communication link, and is used for the communication link with a fixed station 2, The key of the key information DB6, and the transmit information of DB4 for a communication link and the key information DB6 that the key information containing the key (symmetry key) used for the key management processing section 5, the encryption, or the decryption which updates key information

on the key information DB6 (a key is included) is stored is read. The encryption processing section 7 which makes transmit information a cipher, the communications processing section 8 which transmits this cipher to a channel 3 and receives a cipher from a channel 3 again, and the cipher received from the channel 3 are decoded using the key of the key information DB6. It consists of the decryption processing section 9 which stores the receipt information of the decrypted plaintext in DB4 for a communication link, and the control processing section 10 which controls starting of these each part.

[0031] A fixed station 2 A cipher from a channel 3 The communications processing section 8 which receives or transmits, the decode processing section 9 which decrypts the received cipher using the key read from the key information DB13 from the transmitting way 3, DB11 for a communication link which stores the decrypted receipt information and the transmit information of a plaintext, and all the key information supported by the cryptocommunication of a fixed station 2 The receipt information of a mobile station 1 is read from the key information management DB12 to store, the key information DB13 which stores the key used for every mobile station under communication link, and DB11 for a communication link. Contrast the key related information from a mobile station 1, and the key information registered into the key information management DB12, and effective/invalid of the key of a mobile station are judged. The key used stored in the key supervisory control processing section 14 which stores in DB11 for a communication link the key related information which answers a mobile station according to a judgment result, and the key information DB13 is used. It consists of the encryption processing section 7 which enciphers the transmit information which transmits to a mobile station, and the control processing section 16 which starts processing of these each part.

[0032] Below, the example by the symmetry key cipher system explains actuation of each part to a detail. The configuration of the key information database of a mobile station is shown in drawing 2. In the case of a symmetry key cipher system, the key information stored in the key information DB6 consists of effective flags 24 which show effective/invalid of the key (symmetry key) 23 used for the key application 22, the encryption, or the decryption which shows the usual or urgent application of the key version 21 which a mobile station uses, and a symmetry key, and the symmetry key 23. An "urgent" key "K1'" is registered [a key application] into a version "V1" for a usual key "K1" and a "usual" key application, and the example of illustration is both "effective."

[0033] The configuration of the key management information database of a fixed station is shown in drawing 3. The key information management DB12 consists of effective flags 24 which show the hysteresis of one or more key versions which a fixed station 2 supports, usually reach every key version 21 and show effective/invalid of the urgent key application 22 and an urgent key (symmetry key) 23, and a symmetry key. The symmetry key K2 and K2' are registered into a version V1 by the symmetry key K1, K1', and the version V2, and the example of illustration is supported effectively altogether.

[0034] The configuration of the key information database of a fixed station is shown in drawing 4. The key information management DB13 manages correspondence of the key 32 (key 23) used used for the communication link with the mobile station identifier 31 which received from the mobile station under communication link, and this mobile station in order of reception. Correspondence of the mobile station which reception ended is eliminated from DB13, and the order of management is updated. Thereby, the communication link by version which is different from two or more mobile stations in coincidence is attained.

[0035] The flow of key decision processing of the symmetry key cipher system in a mobile station used is shown in drawing 5. The key management processing section 5 makes the key decision of a mobile station 1 under the control processing section 10 at the time of communication link initiation with a fixed station 2, and the processing at the time of a communication link and renewal of key urgent is usually included.

[0036] The key management processing 5 reads the key version currently supported from the key information DB6 (S101), and writes this version in the area of the key related information of DB4 for a communication link (S102). With the message (the identification information of a mobile station is included) of a communication link demand, key related information (here key version) is transmitted to a fixed station 2 from the communications processing section 8. Then, the key management processing 5 waits for reception of the key related information from a fixed station 2 (S103). The key related information (here, they are a key version and a key application) which received from the fixed station 2 is read from DB4 for a communication link (S104), and it judges whether the key version is supported by the local station (S105). When the key version from a fixed station 2 is not supported by the local station, the notice of abnormalities is published to the control processing section 10 (S106), and processing is ended.

[0037] When in agreement with the key version which transmitted from the local station when the key version from a fixed station 2 is supported by the local station that is, it judges whether the key application 22 from a fixed station 2 is urgent (S107). Since a key application is "usual" if not urgent, it is the usual communication link which uses the usual key of a local station, and processing is ended as it is. On the other hand, since the usual key of a local station cannot be used when the key application 22 from a fixed station is "urgent", while using the key used as an urgent key, the effective flag 24 of the usual key in the key information DB6 is updated to an invalid (S108). Consequently, an urgent key is used for encryption/decryption of henceforth in the mobile station concerned.

[0038] The flow of the key decision processing used in a fixed station is shown in drawing 6. The key supervisory control processing section 14 in which the fixed station 2 was started by the control processing section 15 to the communication link demand from a mobile station 1 determines the key used for every mobile station with a symmetry key cipher system.

[0039] The key supervisory control processing 14 reads the version of the key related information which received

with the communication link demand from a mobile station 1 from DB11 for a communication link (S201), and checks the support of the key version which searched the key information management DB12 and received. That is, it judges whether the usual key of the version of a mobile station 1 is effective, or an urgent key is still more effective, if it judges and the key is usually invalid (S202).

[0040] When the usual key of the version which received is effective, this usual key is determined as the key used, and it matches with the identifier of the mobile station concerned, and registers to the key information DB13 (S203). Furthermore, a key application (usually) is added to the key version which received from the mobile station 1 previously as key related information which transmits to a mobile station 1, it writes in DB11 for a communication link (S206), and processing is ended. Moreover, a key is usually invalid, and when an urgent key is effective, the urgent key of the key version which received is determined as the key used (S204), and it registers to the key information DB13.

[0041] Furthermore, when both the usual keys and urgent keys of a key version that were received are invalids, a mobile station is usually answered in the key version currently supported by the fixed station 2, version of the key used which selected the key in the lock used (S205), and selected, and key application. When the mobile station is supporting the version from a fixed station, it is resending this version with a communication link demand, and a series of above-mentioned processings are repeated, the usual key of the version concerned is determined as key used, and a communication link becomes possible.

[0042] However, management which supports the only version is performed and the usual mobile station makes the earlier version the invalid with updating to an upgrade product. In such a case, it judges with key decision processing of a mobile station 1 having no support (S105), and a communication link is closed. Therefore, when both the symmetry keys of the key version which received from the mobile station, without performing processing S205 are invalids, a dummy version may be made to only answer in key decision processing of a fixed station 2.

[0043] The flow of processing between the mobile station in the case of usually determining the key used as drawing 7 by communication link and a fixed station is shown. From ** key information DB6, the key management processing section 5 of a mobile station 1 reads that the key version which a local station supports is V1, and transmits a version V1 to the ** fixed station 2 with the message (Nxx1 containing an identifier) of a communication link demand. ** The key supervisory control processing section 14 of a fixed station 2 searches the key management information DB12 using the version V1 which received from the mobile station 1, and checks whether the version V1 is supported. ** If the support of a version V1 is checked, the usual key K1 of a version V1 will be determined as the key used, and it will match with the identifier (Nxx1) of the mobile station concerned, and will register to the key information DB13. moreover, ** — the key related information which consists of a version V1 and a key application (usually) is transmitted to the mobile station concerned. In addition, key related information may be enciphered by communication link [for the key decision of a mobile station 1 and a fixed station 2] **, and **.

[0044] The key management processing section 5 of a mobile station 1 checks the version V1 and use of the usual key K1 of a local station by the key related information from a fixed station 2. Next, the ** mobile station 1 reads the transmit information of a plaintext into the cipher-processing section 7 from DB4 for a communication link, and enciphers it using the key K1 used read from the key information DB6. For example, in the ETC system of a turnpike, an IC card number, a balance frame, etc. for tariff dropping [lengthen] are enciphered and transmitted. And a cipher is transmitted to a fixed station 2 from ** communications processing section 8. ** The decode processing section 9 of a fixed station 2 decodes the received cipher to a plaintext with the key K1 corresponding to the identifier (Nxx1) of the key information DB13.

[0045] Since according to this it is only the processing which determines the key used between fixed stations by the communication link demand of a mobile station and the communication link between both can begin immediately, communication link time amount can apply also to the ETC system of the turnpike restricted to about 0.1 or less seconds. Moreover, the key used itself used for encryption/decryption is not included in key related information, but since it does not communicate, the high security of a system is securable.

[0046] The flow of processing between the mobile station in the case of determining the key used as drawing 8 by renewal of key urgent and a fixed station is shown. The key management processing section 5 of a mobile station 1 is usually the same as that of the case of a communication link until it reads the version V1 by which effective management is carried out to ** key information DB6, it transmits to the ** fixed station 2 with a Request-to-Send message and the key supervisory control processing section 14 of the ** fixed station 2 checks the support of a version V1. ** the result of a check — the usual key K1 of a version V1 — invalid and urgent key K1' — case it is effective — urgent key K1' of a version V1 — the key used — determining — the identifier (Nxx1) of the mobile station concerned — matching — the key information DB13 — registering — ** — transmit the key related information which consists of a version V1 and a key application (urgent) to the mobile station concerned.

[0047] The key management processing section 5 of a mobile station 1 will make an invalid the effective flag of the usual key K1 of the key information DB6, if the invalid of the usual key K1 of a local station is got to know by the key application from the ** fixed station 2. The cipher-processing section 7 uses K1' effectively managed for the key information DB6 on the occasion of encryption of a plaintext. After transmission (**) of the cipher from a mobile station 1 to a fixed station 2, it is usually the same as that of the case of a communication link. In addition, if a key application is included in a fixed station 2 with a key version from a mobile station 1 at the key related information of a communication link demand, the key decision processing by the side of the fixed station which is using the urgent key can be simplified. At this time, the key related information which answers from a fixed station 2 to a mobile station 1 is good only at a key version.

[0048] By the way, management of effective/invalid of a key is usually performed from high order equipment by the invalid directions to the specific key version in a fixed station. That is, by the central apparatus which liquidate the use tariff of a mobile station etc., when the fact of impossible instantaneous use was physically detected from two or more fixed stations to one mobile station, or when there is a complaint statement from a user, it judges that the unauthorized use occurred and the invalid of a key is usually directed.

[0049] The processing flow of nullification of the usual key in a fixed station is shown in drawing 9. The key supervisory control processing section 14 usually has the processing facility of key nullification besides the processing facility (drawing 6) of the communication link key decision mentioned above. First, it waits for reception of the key application modification directions from high order equipment (S301). If modification directions of the key application which specified the key version are received from high order equipment, the usual key of the specified version will be made into an invalid, and the effective flag concerned of the key information management DB12 will be set as an invalid (S302). In addition, this processing may be processed by interruption to key decision processing.

[0050] Since a change in the urgent lock which makes an invalid the usual key of a key version with which the unauthorized use was revealed, and each mobile station holds can be processed on-line according to this example, the usual employment of a system is maintainable, preventing expansion of the damage by unauthorized use. moreover — since the data of an urgent key are changed without communicating mutually — high — security correspondence is attained.

[0051] For example, in the ETC system of a turnpike, since the renewal of a version of the usual mobile station serves as the time of constant ** etc., there is a possibility that it may be driven into a system stop by expansion of the damage depended unjustly. However, according to this example, since automatic processing of the change in an urgent lock is usually carried out on-line during the communication link of use, a system and a user do not have a burden and it is user-friendly.

[0052] Although the symmetry key was used for the cryptographic key of the cryptocommunication of a mobile station and a fixed station in the above example, the mobile communication of this invention is realizable for a cryptographic key with an unsymmetrical key or the algorithm key into which cryptographic algorithm is changed.

[0053] Moreover, in the symmetry key cipher system mentioned above, the symmetry key which usually becomes a mobile station and a fixed station from a key and an urgent key beforehand is prepared. However, the fixed station usually installs only the key, and it is added to the key application modification directions to a fixed station from high order equipment, and you may make it transmit the urgent key of the version concerned. Thereby, discovery of the urgent key by the theft in a fixed station etc. can be prevented. In addition, since the risk of leakage by the communication link of the key information from high order equipment follows, it considers as temporary immediate steps, and the renewal of a version of a mobile station is radically needed.

[0054]

[Effect of the Invention] Since according to the mobile correspondence procedure of this invention the version of the communication link demand of a mobile station is checked and the key used can be determined for fixed-station itself when sharing two or more versions of a common key with a fixed station and two or more mobile stations, the communication link with a mobile station can be started promptly.

[0055] Moreover, since the efficiency of the change in the alternative lock which each mobile station holds can be carried out in on-line processing, without transmitting a cryptographic key when an unauthorized use is revealed, since a symmetry key cipher system is adopted, expansion of the damage of an unauthorized use can be prevented.

[0056] High security is securable while a system configuration simplifies, since a key server is made unnecessary according to the mobile communication system of this invention. Moreover, since automatic processing of the key switch in emergency is carried out while communicating, it is user-friendly.

[Translation done.]

* NOTICES *

JPO and NCIP are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.*** shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] The block diagram of the mobile communication system by one example of this invention.

[Drawing 2] The data block diagram of the key information DB on the mobile station using a symmetry key cipher system.

[Drawing 3] The data block diagram of the key management information DB of a fixed station using a symmetry key cipher system.

[Drawing 4] The block diagram of the key information DB which manages the key used under message of a fixed station.

[Drawing 5] The flow Fig. showing decision processing of the key used by the symmetry key cipher system of a mobile station.

[Drawing 6] The flow Fig. showing decision processing of the key used by the symmetry key cipher system of a fixed station.

[Drawing 7] The explanatory view showing processing and data flow of the usual key decision between a mobile station and a fixed station.

[Drawing 8] The explanatory view showing processing and data flow of renewal of key urgent between a mobile station and a fixed station.

[Drawing 9] The flow Fig. showing usual key nullification processing of a fixed station with high order directions.

[Drawing 10] The block diagram of the outline of the electronic toll collection system (ETC) of a turnpike.

[Drawing 11] The explanatory view of the conventional mobile communication system in which the key decision actuation by the key server inquiry is shown.

[Description of Notations]

1 [— DB for a communication link 5 / — Key management processing section,] — A mobile station, 2 — A fixed station, 3 — A channel, 4 6 — The key information DB (mobile station side), 7 — The encryption processing section, 8 — Communications processing section, 9 — The decryption processing section, 10 — The control processing section (mobile station side), 11 — DB for a communication link, 12 — The key information management DB, 13 — The key information DB (fixed-station side), 14 — Key supervisory control processing section, 16 [— A symmetry key, 24 / — An effective flag, 31 / — A mobile station identifier, 32 / — The key used, 100 / — A fixed station, 110 / — An antenna, 200 / — An exclusive lane, 210 / — A communications area, 300 / — A car, 310 / — Mobile station.] — The control processing section (fixed-station side), 21 — A key version, 22 — A key application, 23

[Translation done.]

* NOTICES *

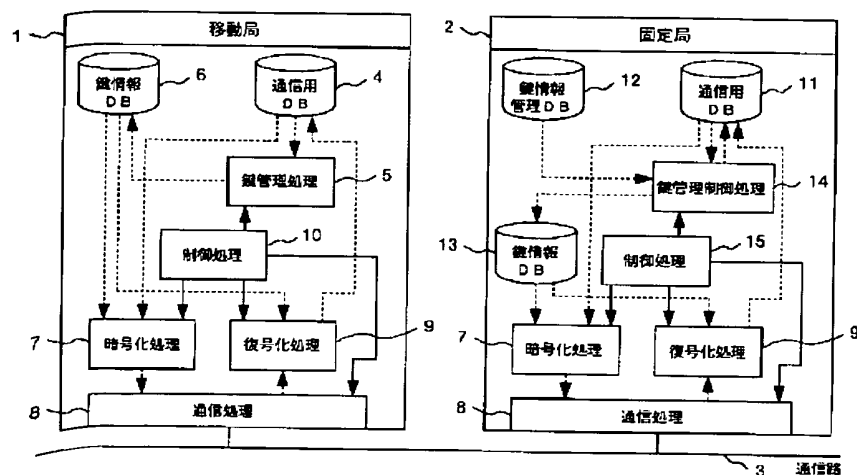
JPO and NCIP are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. *** shows the word which can not be translated.
3. In the drawings, any words are not translated.

DRAWINGS

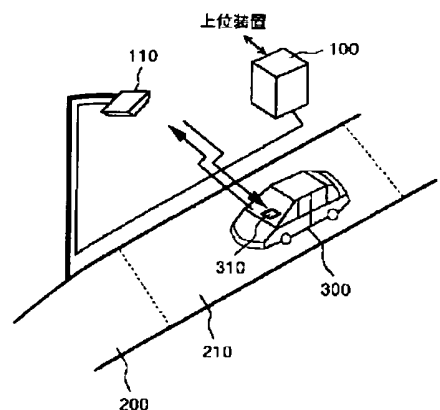
[Drawing 1]

図 1



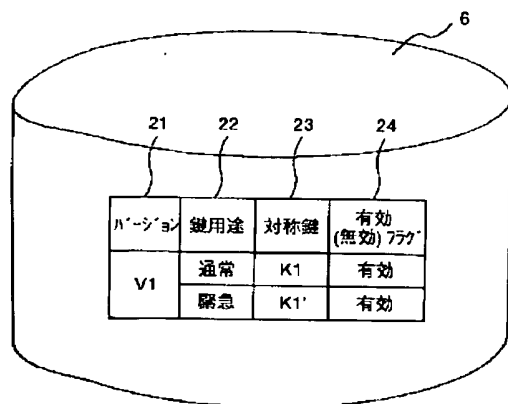
[Drawing 10]

図 10



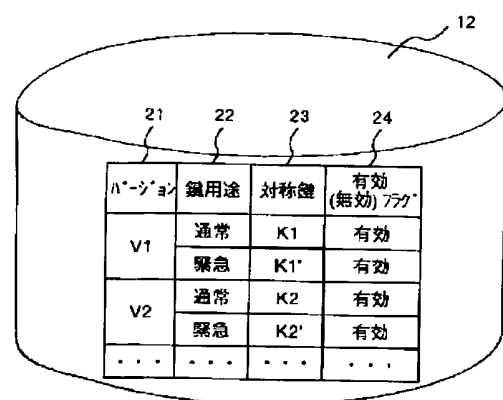
[Drawing 2]

図 2



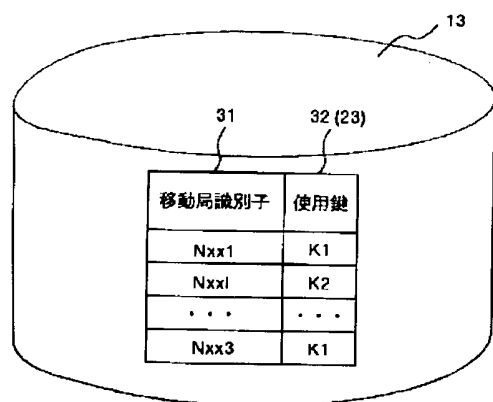
[Drawing 3]

図 3



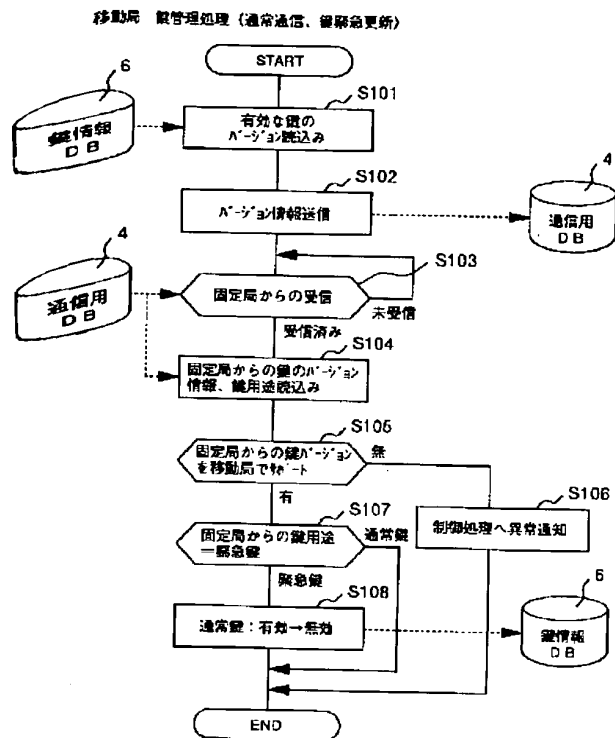
[Drawing 4]

図 4



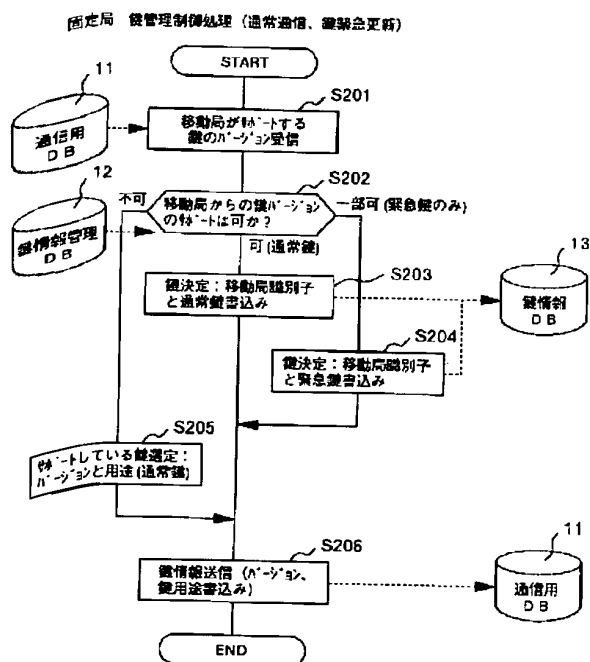
[Drawing 5]

図 5



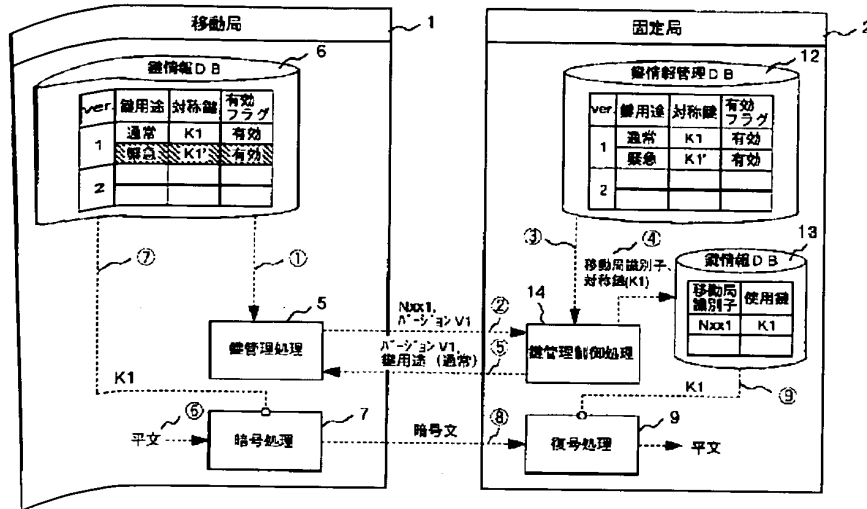
[Drawing 6]

図 6



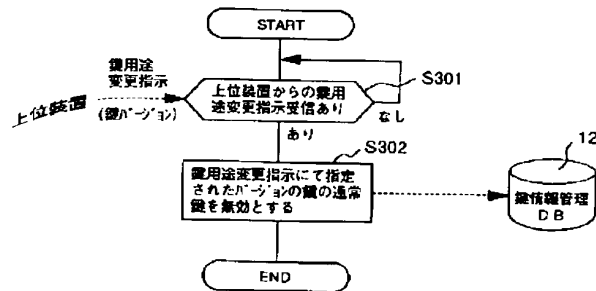
[Drawing 7]

図 7



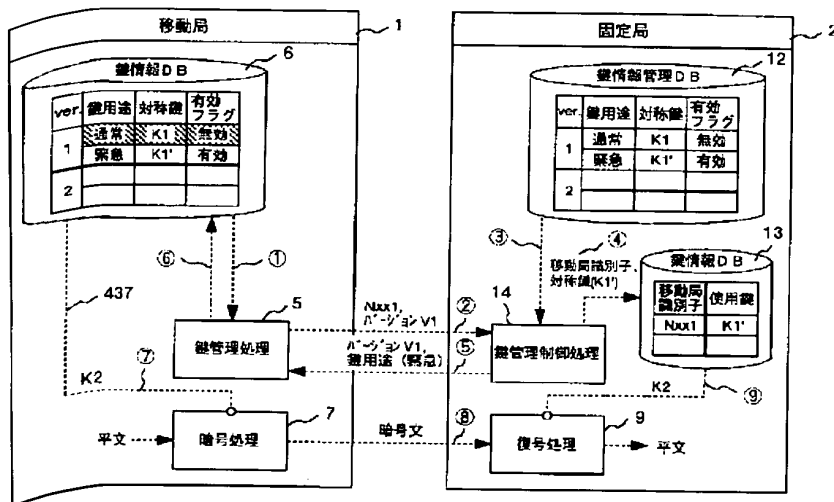
[Drawing 9]

図 9



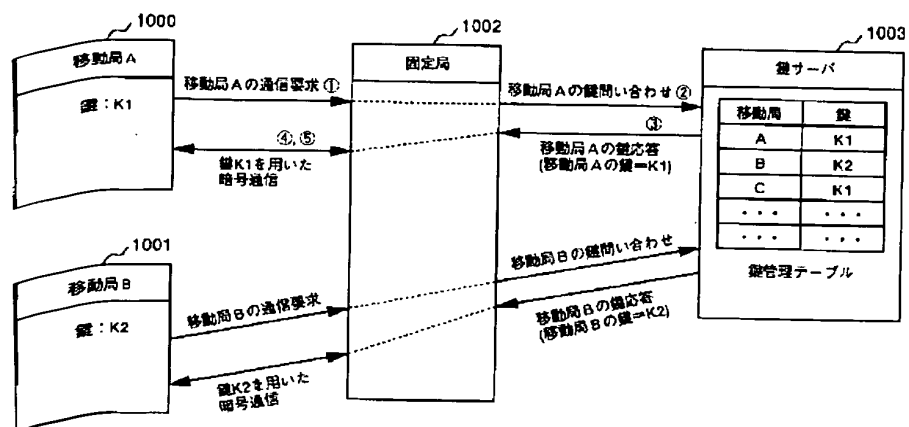
[Drawing 8]

図 8



[Drawing 11]

図 1 1



[Translation done.]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-274999

(43) 公開日 平成11年(1999)10月8日

(51) Int.Cl. ⁶	識別記号	F I	
H 0 4 B 7/26		H 0 4 B 7/26	R
G 0 7 B 15/00		G 0 7 B 15/00	J
			H
	5 1 0		5 1 0
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 E
審査請求 未請求 請求項の数10 OL (全 11 頁) 最終頁に続く			

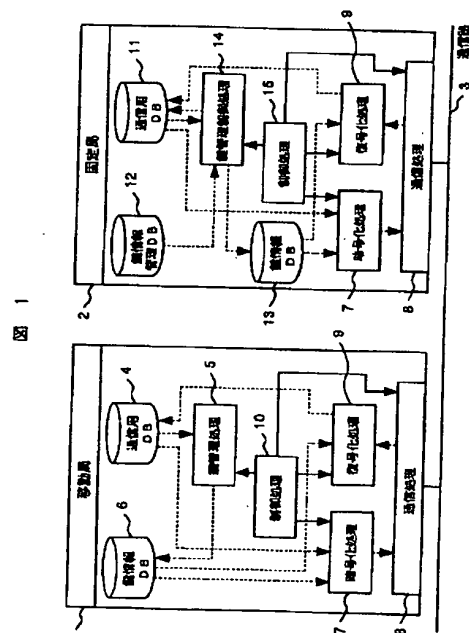
(21) 出願番号	特願平10-76909	(71) 出願人	000005108 株式会社日立製作所 東京都千代田区神田駿河台四丁目6番地
(22) 出願日	平成10年(1998)3月25日	(71) 出願人	000153443 株式会社日立情報制御システム 茨城県日立市大みか町5丁目2番1号
		(72) 発明者	野里 雅哉 茨城県日立市大みか町五丁目2番1号 株式会社日立情報制御システム内
		(72) 発明者	粥川 悟 茨城県日立市大みか町五丁目2番1号 株式会社日立情報制御システム内
		(74) 代理人	弁理士 高橋 明夫 (外1名) 最終頁に続く

(54) 【発明の名称】 移動体通信方法および移動体通信システム

(57) 【要約】

【課題】 移動局と固定局間の通信開始を高速化し、また暗号鍵の不正使用等に対し速やかに且つ安全に使用鍵を切り替える移動体通信方式を提供する。

【解決手段】 固定局と複数の移動局間の暗号通信に、複数のバージョンによる共通鍵を使用可能とし、各々の移動局1は唯一の鍵バージョンとその対称鍵（通常鍵と緊急鍵）を鍵情報DB6に管理し、固定局2は複数の鍵バージョンとその対称鍵を鍵情報管理DB12に管理する。移動局1は通信要求時に自局の鍵バージョンを送信し、固定局2は受信した鍵バージョンの通常鍵が有効にサポートされているか判定し、有効な場合は当該バージョンと鍵用途（通常）を応答する。また、通常鍵が無効な場合は、当該バージョンと鍵用途（緊急）を応答する。移動局1は固定局2から応答された鍵バージョンと鍵用途を判定し、鍵バージョンが同じでも鍵用途が「緊急」の場合は、自局の使用鍵を緊急鍵に切り替える。



【特許請求の範囲】

【請求項1】 固定局と移動局との双方向の暗号通信の暗号化または復号化に用いる鍵（暗号鍵）を複数の移動局で共有可能とし、かつ前記鍵の複数のバージョンを共用可能とする移動体通信方法において、

移動局は固定局への通信要求時に、自局の使用可能な暗号鍵のバージョンを送信すると共に、このバージョンが固定局からの応答に含まれることを確認し、

固定局は移動局からの受信バージョンが自局の管理する鍵情報に含まれるかチェックし、含まれる場合は当該バージョンを使用鍵に決定して前記通信要求を発信した移動局に回答すると共に、通信中、当該移動局の識別子とその使用鍵を対応付けて管理することを特徴とする移動体通信方法。

【請求項2】 請求項1において、

固定局は、移動局からの受信バージョンが自局の管理する鍵情報に含まれていない場合は、有効な鍵情報の一つまたはダミーのバージョンを移動局に回答し、当該移動局は、固定局からの応答バージョンが自局で使用可能な場合はそれによる通信要求を再送信することを特徴とする移動体通信方法。

【請求項3】 固定局と移動局との双方向の暗号通信の暗号化または復号化に用いる暗号鍵を複数の移動局で共有可能とし、かつ前記暗号鍵の複数のバージョンを共用可能とする移動体通信方法において、各移動局及び固定局はそれぞれ自局の使用可能なバージョンの暗号鍵を、通常用と代替用の鍵用途に対応した一対の鍵（通常鍵と代替鍵）により管理し、

移動局は固定局への通信要求時に、自局の使用可能な暗号鍵のバージョンを送信すると共に、固定局からの応答に含まれるバージョンと鍵用途をチェックし、応答のバージョンが自局と同一で鍵用途が通常用の場合は、自局の通信に使用する暗号鍵を前記通常鍵のままとし、固定局は移動局からの受信バージョンが自局の管理する複数のバージョンに含まれるかチェックし、含まれる場合は前記通常鍵の有効／無効をチェックし、有効の場合は当該通常鍵を使用鍵に決定して当該バージョンと鍵用途（通常用）を前記通信要求を発信した移動局に回答すると共に、通信中、当該移動局の識別子とその使用鍵を対応付けて管理することを特徴とする移動体通信方法。

【請求項4】 請求項3において、

固定局は、移動局からの受信バージョンが自局の管理するバージョンに含まれかつ前記通常鍵が無効の場合に、当該通常鍵と対をなす代替鍵を使用鍵に決定して当該バージョンと鍵用途（代替用）を前記通信要求を発信した移動局に回答すると共に、通信中、当該移動局の識別子とその使用鍵を対応付けて管理し、

当該移動局は、固定局から応答の鍵用途が代替用の場合に、自局の通常鍵を無効とし、それと対をなす代替鍵を自局の暗号通信の使用鍵とすることを特徴とする移動体

通信方法。

【請求項5】 固定局と移動局との双方向の暗号通信の暗号化または復号化に用いる暗号鍵を複数の移動局で共有可能とし、かつ前記暗号鍵の複数のバージョンを共用可能とする移動体通信方法において、

各移動局及び固定局はそれぞれ自局の使用可能なバージョンの暗号鍵を、通常用と代替用の鍵用途に対応した一対の鍵（通常鍵と代替鍵）により管理し、

移動局は固定局への通信要求時に、自局の使用可能な暗号鍵のバージョンと鍵用途（通常または代替）を送信すると共に、固定局からの応答に含まれるバージョンをチェックし、応答のバージョンが自局と同一の場合は、自局から送信した鍵用途の暗号鍵を使用し、

固定局は移動局から受信したバージョンが自局の管理する複数のバージョンに含まれる場合に、受信した鍵用途が通常であれば前記通常鍵の有効／無効をチェックし、有効の場合は通常鍵を、無効の場合は前記代替鍵を使用鍵に決定し、受信したバージョンを前記通信要求を発信した移動局に回答すると共に、通信中、当該移動局の識別子とその使用鍵を対応付けて管理することを特徴とする移動体通信方法。

【請求項6】 請求項3、4または5において、

固定局における前記通常鍵の有効／無効の管理は、上位装置から指定されたバージョンの鍵用途変更指示を受信したときに、当該通常鍵を無効とすることを特徴とする移動体通信方法。

【請求項7】 通信処理手段と暗号化・復号化処理手段を有する固定局と、移動体上に搭載され通信処理手段と暗号化・復号化処理手段を有する複数の移動局を備え、移動局と固定局の双方向の暗号通信に用いる暗号鍵を複数の移動局で共有可能とし、かつ前記暗号鍵の複数のバージョンを共用可能とする移動体通信システムにおいて、

移動局は、自局の通信に使用する鍵バージョンと鍵を含む鍵情報を格納する鍵情報データベースと、固定局への通信要求時に自局の鍵バージョンを送信すると共に、固定局からの応答に含まれる鍵バージョンと対照して自局の使用鍵を管理する鍵管理処理手段を設け、

固定局は、移動局との通信に使用する複数の鍵バージョンとその鍵を含む鍵情報を格納する鍵情報管理データベースと、移動局から受信した鍵バージョンが前記鍵情報管理データベースに含まれる場合に当該鍵バージョンの鍵を使用鍵に決定して、当該鍵バージョンを移動局に回答する鍵管理制御処理手段と、通信中の移動局の識別子とその使用鍵を対応付けて管理する通信鍵情報データベースを設けることを特徴とする移動体通信システム。

【請求項8】 請求項7において、

固定局及び移動局は、前記鍵情報として鍵バージョン毎に通常／代替の鍵用途と対応する一対の通常鍵と代替鍵を含み、かつ固定局には、上位からの鍵用途変更指示に

よって該当鍵バージョンの通常鍵の使用を無効にする管理機能を有し、

固定局の前記鍵管理制御処理手段は、移動局から受信した鍵バージョンの通常鍵が無効の場合に對の代替鍵を使用鍵に決定してその鍵バージョンと鍵用途（代替）を移動局に伝達し、移動局の前記鍵管理制御処理手段は固定局から伝達された鍵用途が代替用の場合に鍵情報データベースの通常鍵を無効にすることを特徴とする移動体通信システム。

【請求項9】 請求項7において、

移動局は前記鍵情報として鍵バージョン毎に通常／代替の鍵用途と対応する一対の通常鍵と代替鍵を含み、固定局は前記鍵情報として鍵バージョン毎に通常鍵の鍵用途となる通常鍵を含み、かつ上位から鍵用途変更指示による鍵バージョンと鍵用途が代替の代替鍵を受信して管理すると共に当該通常鍵の使用を無効にする管理機能を有し、固定局の前記鍵管理制御処理手段は、移動局から受信した鍵バージョンの通常鍵が無効の場合に前記代替鍵を使用鍵に決定してその鍵バージョンと鍵用途（代替）を移動局に伝達し、移動局の前記鍵管理制御処理手段は固定局から伝達された鍵用途が代替用の場合に鍵情報データベースの通常鍵を無効にすることを特徴とする移動体通信システム。

【請求項10】 請求項7、8または9において、前記移動体通信システムは有料道路の自動料金収受システムであり、前記固定局は料金所または路側に設けられる通信装置、前記移動局は有料道路を利用する車両に搭載される通信装置により構成される移動体通信システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は暗号通信方法に関し、特に固定局と移動局間で秘密にかつ耐改竄に暗号鍵を管理する移動通信に関する。

【0002】

【従来の技術】携帯電話や自動車電話による移動通信の普及がめざましく、有料道路の自動料金収受システム（ETC）などの実用化も間近である。有料道路の自動料金収受システムは、料金所路側に設置された固定通信手段（固定局）と有料道路を走行する車両に搭載された移動通信手段（移動局）の間で、無線通信を用いて料金を収受するシステムである。ETCの課金処理では、利用者の認証や預金情報など個人のプライバシーに関する情報を無線で送受信するので、これら情報の漏洩、改竄を防止するために暗号通信を用いたセキュリティの確保が必須となる。

【0003】通信内容の秘密保持や改竄の防止のために、平文を暗号化し暗号文を復号化するための鍵情報が使用される。例えば、「インターネットセキュリティ

」基礎と対策技術（佐々木良一他著、オーム社、pp 95-102）」に記載のように、送信者と受信者間で予め、KEK(Key Encrypting Key)と呼ばれる「鍵暗号化鍵」を設定し、送信者はこのKEKを用いてデータを暗号化するDEK(Data Encrypting Key)と呼ばれる

「データ暗号化鍵」を暗号化して受信者へ送信し、受信者はKEKを用いてDEKを復号化し、DEKを用いて暗号文を解読している。

【0004】また、送信者は受信者の公開鍵を入手し、この公開鍵をKEKとして暗号化したDEKを受信者へ送付し、送信者と受信者との間でDEKを共有する方法もある。これら暗号化鍵の管理はカードによる方法もあるが、鍵情報の変質や紛失の危険もある。一般には、鍵サーバによって移動局毎に管理している。

【0005】図11に、鍵サーバを使用する移動局と固定局の暗号通信の手順を示す。鍵サーバは鍵管理テーブルに移動局Aの鍵K1、移動局Bの鍵K2と、全移動局の鍵を管理している。鍵K1を保持している移動局Aが固定局と通信する場合、①移動局Aの識別子による通信要求を発行し、②固定局は鍵サーバに移動局Aの鍵を問合せ、③鍵サーバは固定局に移動局Aの鍵K1を伝達し、④固定局は鍵K1（またはデータK1を種に生成した鍵K11）を用いて移動局Aに暗号通信を行ない、⑤移動局Aは鍵K1（またはデータK1から解読した鍵K11）を用いて暗号文を復号し、鍵K1（または鍵K11）を用いた暗号文で固定局と通信する。

【0006】なお、鍵情報は漏洩（盗聴・解読）による不正使用を防止するために、定期的または必要に応じてバージョンアップされる。鍵サーバが管理する鍵情報は移動局に固有の鍵または移動局に共通の鍵で、後者の場合は移動局毎に使用中の鍵バージョンが管理される。つまり、図9に例示した鍵K1、K2は固有情報でも、バージョン情報でもよい。

【0007】

【発明が解決しようとする課題】上述のように、暗号通信の鍵情報を鍵サーバによって管理する方式では、固定局は移動局からの通信要求の度に使用する鍵をサーバに問合せするので、移動局と固定局間の通信開始までに時間がかかり、またサーバから固定局へKEKやDEKの鍵情報を直接に送信するので漏洩の危険も高い。

【0008】特に、ETCでは料金収受に用いる無線電波の混信を防ぐために、通信領域を狭く設定する必要がある。一方、自動料金収受を行なう車両は停止することなく料金所を通過させる運用となるので、固定局と移動局との間の通信可能な時間はごく短い。例えば、車両が4mの通信領域を180km/hの高速で走行した場合、通信可能な時間はわずか80msである。従って、サーバによる鍵管理方式では、車両と料金所間の高速応答が困難なため、高速通過による料金収受が不可能になるので、料金所での渋滞解消に役立たなくなる。

【0009】しかし、不特定多数の移動局の鍵情報をサーバに代わって固定局が管理することは、従来の技術では不可能である。なぜならば、個々の移動局が全国のどの料金所へ進入して通信を開始するか分からないので、各固定局は全移動局の鍵情報の管理が必要になるからである。移動局が共通鍵を使用する場合でも、移動局の鍵バージョンは個々の車検時などに更新されるので、複数の鍵バージョンを共用可能に運用する必要があり、固定局の管理は困難となる。

【0010】また、使用中の鍵バージョンに不正使用が発覚した場合、被害のあった移動局への緊急対策はできても、その鍵バージョンを使用している他の多数の移動局に対しては緊急に対応できず、被害の拡大する恐れがある。

【0011】本発明の目的は、従来の暗号文を含む移動通信の問題点を克服し、鍵情報の漏洩の危険が少なく高応答で通信を開始でき、あるいは緊急時の鍵更新が簡単に行なえる移動通信方法を提供することにある。

【0012】また、鍵サーバの不要なシンプルで、高セキュリティの移動通信システムを提供することにある。さらに、短時間（高速通過中）に確実に料金収集（課金処理）のできる有料道路の自動料金収受システムを提供することにある。

【0013】

【課題を解決するための手段】上記目的を達成するための本発明は、固定局と移動局の双方向の暗号通信の暗号化または復号化に用いる鍵（暗号鍵）を複数の移動局で共有可能とし、かつ前記暗号鍵の複数のバージョンを共用可能とする移動体通信方法において、移動局は固定局への通信要求時に、自局の使用可能な暗号鍵のバージョンを送信すると共に、このバージョンが固定局からの応答に含まれることを確認し、固定局は移動局からの受信バージョンが自局の管理する鍵情報に含まれるかチェックし、含まれる場合は当該バージョンを使用鍵に決定して前記通信要求を発信した移動局に応答すると共に、通信中、当該移動局の識別子とその使用鍵を対応付けて管理することを特徴とする。

【0014】上記の固定局は、移動局からの受信バージョンが自局の管理する鍵情報に含まれていない場合は、鍵情報の一つまたはダミーのバージョンを移動局に応答し、当該移動局は、固定局からの応答バージョンが自局で使用可能な場合は、この応答のバージョンを使用鍵として、通信要求を再送信することを特徴とする。この結果、再送のバージョンが固定局で使用鍵に認められ、通信中管理される。

【0015】この発明によれば、固定局は複数の移動局との間で、共通鍵の複数の鍵バージョンを混乱なく共用でき、固定局自身で使用鍵を決定できるので、即座に通信を開始できる。

【0016】また、本発明は、各移動局及び固定局がそ

れぞれ自局の使用可能なバージョンの暗号鍵を、通常用と代替用の鍵用途に対応した一対の鍵（通常鍵と代替鍵）により管理し、移動局は固定局への通信要求時に、自局の使用可能な暗号鍵のバージョンを送信すると共に、固定局からの応答に含まれるバージョンと鍵用途をチェックし、応答のバージョンが自局と同一で鍵用途が通常用の場合は、自局の通信に使用する暗号鍵を前記通常鍵のままとし、固定局は移動局からの受信バージョンが自局の管理する複数のバージョンに含まれるかチェックし、含まれる場合は前記通常鍵の有効／無効をチェックし、有効の場合は当該通常鍵を使用鍵に決定して当該バージョンと鍵用途（通常用）を前記通信要求を発信した移動局に応答すると共に、通信中、当該移動局の識別子とその使用鍵を対応付けて管理することを特徴とする。

【0017】また、上記の固定局は、移動局からの受信バージョンが自局の管理するバージョンに含まれかつ前記通常鍵が無効の場合に、当該通常鍵と対をなす代替鍵を使用鍵に決定して当該バージョンと鍵用途（代替用）を前記通信要求を発信した移動局に応答すると共に、通信中、当該移動局の識別子とその使用鍵を対応付けて管理し、当該移動局は、固定局から応答の鍵用途が代替用の場合に、自局の通常鍵を無効とし、それと対をなす代替鍵を自局の暗号通信の使用鍵とすることを特徴とする。

【0018】さらに、上記の固定局における前記通常鍵の有効／無効の管理は、上位装置から指定されたバージョンの鍵用途変更指示を受信したときに、当該通常鍵を無効とすることを特徴とする。

【0019】この発明によれば、不正使用が発覚した場合等に鍵バージョンの通常鍵を無効にし、各移動局が保持している代替鍵への切り替えを、暗号鍵を送信することなく通信中のオンライン処理できるので、緊急な対応が高セキュリティに実行できる。なお、通常鍵と代替鍵（実施例では緊急鍵）の対による方式を、以下では対称鍵暗号方式と呼ぶ。

【0020】なお、上記で移動局から通信要求時に自局で使用する鍵のバージョンと鍵用途を送信し、固定局で使用を決定したバージョンのみを応答するようにしてもよい。これによれば、固定局の鍵決定処理がさらに簡素化される。

【0021】上記移動体通信方法を適用する本発明の移動体通信システムは、固定局と移動体上に搭載される複数の移動局を備え、移動局は、自局の通信に使用する鍵バージョンと鍵を含む鍵情報を格納する鍵情報データベースと、固定局への通信要求時に自局の鍵バージョンを送信すると共に、固定局からの応答に含まれる鍵バージョンと対照して自局の使用鍵を管理する鍵管理処理手段を設け、固定局は、移動局との通信に使用する複数の鍵バージョンとその鍵を含む鍵情報を格納する鍵情報管理

データベースと、移動局から受信した鍵バージョンが前記データベースに含まれる場合にこの鍵バージョンの鍵を使用鍵に決定して、当該鍵バージョンを移動局に回答する鍵管理制御処理手段と、通信中の移動局の識別子とその使用鍵を対応付けて管理する通信鍵情報データベースを設けることを特徴とする。

【0022】また、固定局及び移動局は、前記鍵情報として鍵バージョン毎に通常／代替の鍵用途と対応する一対の通常鍵と代替鍵を含み、かつ固定局には、上位からの鍵用途変更指示によって該当鍵バージョンの通常鍵の使用を無効にする管理機能を有し、固定局の前記鍵管理制御処理手段は、移動局から受信した鍵バージョンの通常鍵が無効の場合にその代替鍵を使用鍵に決定してその鍵バージョンと鍵用途（代替）を移動局に回答し、移動局の前記鍵管理制御処理手段は固定局から回答の鍵用途が代替の場合に鍵情報データベースの通常鍵を無効にすることを特徴とする。

【0023】あるいは、固定局は前記鍵情報として鍵バージョン毎に通常の鍵用途となる通常鍵のみを含み、かつ上位から鍵用途変更指示による鍵バージョンと鍵用途が代替の代替鍵を受信して管理すると共に当該通常鍵の使用を無効にする管理機能を有してなることを特徴とする。

【0024】上記の移動体通信システムの一適用例は有料道路の自動料金収受システム（ＥＴＣ）であり、固定局は料金所または路側に設けられる通信装置、移動局は有料道路を利用する車両に搭載される通信装置として構成される。

【0025】本発明の移動体通信システムは鍵サーバを不要とするので、システム構成が簡素化するとともに、高セキュリティを確保できる。また、固定局と移動局間の通信が高速処理できるので、有料道路のＥＴＣの処理時間を短縮し、高速通過での料金収受が可能になる。

【0026】

【発明の実施の形態】以下、本発明の一実施形態による移動通信方法とそのシステムについて、図面を参照しながら詳細に説明する。なお、各図を通して同等の構成要素には同一の符号を付している。

【0027】図10に、本発明を適用する有料道路の自動料金収受システムの概略の構成を示す。料金所に配置されたＥＴＣの固定局100は、自動料金専用レーン200の上部または側部に設置されたアンテナ110を介して、破線で示す通信エリア210内に進入した車両300の搭載する移動局310との間で、秘密情報を暗号化して無線交信し、料金を自動徴収して上位装置へ報告する。

【0028】アンテナ110のカバーする通信エリア210の延長は、他車との混信を防止するために高々数mである。このため、高速で通過する車両の移動局310と約0.1秒以下で交信を終了しなければならず、固定

局100と移動局310間の暗号通信には高速の応答が必要になる。

【0029】図1は、本発明の一実施例による移動通信システムの構成図である。移動体に搭載された通信装置（移動局）1、移動局1と通信する路側に設置された通信装置（固定局）2、移動局1と固定局2を結ぶ通信路3から構成される。通信路3は無線、有線を問わないが、本実施例ではアンテナを介した無線による。以下では、移動局1と固定局2間の暗号通信を説明するが、秘密情報のみを暗号化して平文と組合せる場合も含む。また、暗号化／復号化のための鍵は上述の「データ暗号化鍵（ＤＥＫ）」を指すが、「鍵暗号化鍵（ＫＥＫ）」でもよい。

【0030】移動局1は、平文の送信情報や受信情報及び鍵関連情報（鍵は含まない）を蓄えている通信用ＤＢ4、通信用ＤＢ4に蓄積されている固定局2からの鍵関連情報を読み出し、固定局2との通信に使用する鍵の決定と、鍵情報ＤＢ6の鍵情報（鍵を含む）の更新を行なう鍵管理処理部5、暗号化または復号化に用いる鍵（対称鍵）を含む鍵情報を格納する鍵情報ＤＢ6、通信用ＤＢ4の送信情報と鍵情報ＤＢ6の鍵を読み出し、送信情報を暗号文にする暗号化処理部7、この暗号文を通信路3へ送信した通信路3から暗号文を受信する通信処理部8、通信路3から受信した暗号文を鍵情報ＤＢ6の鍵を用いて復号し、復号化した平文の受信情報を通信用ＤＢ4へ格納する復号化処理部9、これら各部の起動を制御する制御処理部10から構成されている。

【0031】固定局2は、通信路3から暗号文を受信または送信する通信処理部8、送信路3から受信した暗号文を鍵情報ＤＢ13から読み出した鍵を用いて復号化する復号処理部9、復号化された受信情報や平文の送信情報を蓄える通信用ＤＢ11、固定局2の暗号通信でサポートする全ての鍵情報を格納する鍵情報管理ＤＢ12、通信中の移動局毎の使用鍵を格納する鍵情報ＤＢ13、通信用ＤＢ11から移動局1の受信情報を読み出し、移動局1からの鍵関連情報と鍵情報管理ＤＢ12に登録されている鍵情報を対照して移動局の鍵の有効／無効を判定し、判定結果に応じて移動局に回答する鍵関連情報を通信用ＤＢ11へ格納する鍵管理制御処理部14、鍵情報ＤＢ13に格納された使用鍵を用い、移動局に送信する送信情報を暗号化する暗号化処理部7、これら各部の処理を起動する制御処理部16から構成されている。

【0032】以下では、対称鍵暗号方式による実施例によって、各部の動作を詳細に説明する。図2に、移動局の鍵情報データベースの構成を示す。対称鍵暗号方式の場合、鍵情報ＤＢ6に格納される鍵情報は、移動局が使用する鍵バージョン21、対称鍵の通常または緊急の用途を示す鍵用途22、暗号化または復号化に用いる鍵（対称鍵）23、対称鍵23の有効／無効を示す有効フラグ24から構成される。図示例は、バージョン「V

1」に鍵用途が「通常」の鍵「K1」と、鍵用途が「緊急」の鍵「K1'」が登録されて、共に「有効」である。

【0033】図3に、固定局の鍵管理情報データベースの構成を示す。鍵情報管理DB12は、固定局2がサポートする一つ以上の鍵バージョンの履歴を示し、鍵バージョン21毎に通常及び緊急の鍵用途22と鍵（対称鍵）23、対称鍵の有効／無効を示す有効フラグ24から構成されている。図示例は、バージョンV1に対称鍵K1、K1'、バージョンV2に対称鍵K2、K2'が登録され、全て有効にサポートされている。

【0034】図4に、固定局の鍵情報データベースの構成を示す。鍵情報管理DB13は、通信中の移動局から受信した移動局識別子31と、この移動局との通信に用いる使用鍵32（鍵23）の対応を受信順に管理する。受信の終了した移動局の対応はDB13から消去され、管理順が更新される。これにより、同時に複数の移動局と異なるバージョンでの通信が可能になる。

【0035】図5に、移動局における対称鍵暗号方式の使用鍵決定処理のフローを示す。移動局1の鍵決定は固定局2との通信開始時に、制御処理部10の下で鍵管理処理部5が行ない、通常通信時と鍵緊急更新時の処理を含んでいる。

【0036】鍵管理処理5は、鍵情報DB6よりサポートしている鍵バージョンを読み込み（S101）、このバージョンを通信用DB4の鍵関連情報のエリアへ書き込む（S102）。鍵関連情報（ここでは、鍵バージョン）は通信要求のメッセージ（移動局の識別情報を含む）と共に、通信処理部8から固定局2へ送信される。その後、鍵管理処理5は固定局2からの鍵関連情報の受信を待つ（S103）。固定局2から受信した鍵関連情報（ここでは、鍵バージョンと鍵用途）を通信用DB4より読み出し（S104）、その鍵バージョンが自局でサポートされているか判定する（S105）。固定局2からの鍵バージョンが自局でサポートされていない場合は、制御処理部10へ異常通知を発行し（S106）、処理を終了する。

【0037】固定局2からの鍵バージョンが自局でサポートされている場合、つまり自局から送信した鍵バージョンと一致するとき、固定局2からの鍵用途22が緊急か否か判定する（S107）。緊急でなければ鍵用途は「通常」なので、自局の通常鍵を使用する通常通信であり、そのまま処理を終了する。一方、固定局からの鍵用途22が「緊急」の場合は自局の通常鍵が使用できないので、使用鍵を緊急鍵とするとともに鍵情報DB6における通常鍵の有効フラグ24を無効に更新する（S108）。この結果、当該移動局における以後の暗号化／復号化には、緊急鍵が使用される。

【0038】図6に、固定局における使用鍵決定処理のフローを示す。固定局2は移動局1からの通信要求に対

し、制御処理部15に起動された鍵管理制御処理部14が、対称鍵暗号方式によって移動局毎の使用鍵を決定する。

【0039】鍵管理制御処理14は、移動局1から通信要求とともに受信した鍵関連情報のバージョンを通信用DB11より読み出し（S201）、鍵情報管理DB12を検索して受信した鍵バージョンのサポートを確認する。つまり、移動局1のバージョンの通常鍵が有効か判定し、もし通常鍵が無効であればさらに緊急鍵が有効か判定する（S202）。

【0040】受信したバージョンの通常鍵が有効の場合は、この通常鍵を使用鍵に決定し、当該移動局の識別子と対応付けて鍵情報DB13へ登録する（S203）。さらに、移動局1へ送信する鍵関連情報として、先に移動局1から受信した鍵バージョンに鍵用途（通常）を付加して、通信用DB11へ書き込み（S206）、処理を終了する。また、通常鍵が無効で緊急鍵が有効の場合は、受信した鍵バージョンの緊急鍵を使用鍵に決定し（S204）、鍵情報DB13へ登録する。

【0041】さらに、受信した鍵バージョンの通常鍵と緊急鍵が共に無効の場合は、固定局2でサポートしている鍵バージョンとその通常鍵を使用鍵に選定し（S205）、選定した使用鍵のバージョンと鍵用途を移動局に応答する。移動局が固定局からのバージョンをサポートしている場合は、このバージョンを通信要求とともに再送することで、上記の一連の処理が繰り返され、当該バージョンの通常鍵が使用鍵として決定され、通信が可能になる。

【0042】しかし、通常の移動局は唯一のバージョンをサポートする管理が行なわれ、新バージョンへの更新と共に旧バージョンを無効にしている。このような場合には、移動局1の鍵決定処理はサポート無しと判定し（S105）、通信を打ち切る。従って、固定局2の鍵決定処理では処理S205を行わずに、移動局から受信した鍵バージョンの対称鍵が共に無効の場合は、単にダミーのバージョンを応答するようにしてもよい。

【0043】図7に、通常通信で使用鍵を決定する場合の移動局と固定局間の処理の流れを示す。移動局1の鍵管理処理部5は、①鍵情報DB6より自局がサポートする鍵バージョンがV1であることを読み込み、②固定局2へ通信要求のメッセージ（識別子を含む、例えばN×1）と共にバージョンV1を送信する。③固定局2の鍵管理制御処理部14は、移動局1から受信したバージョンV1を用いて鍵管理情報DB12を検索し、バージョンV1をサポートしているか確認する。④バージョンV1のサポートを確認すると、バージョンV1の通常鍵K1を使用鍵に決定し当該移動局の識別子（N×1）と対応付けて鍵情報DB13へ登録する。また、⑤当該移動局へバージョンV1と鍵用途（通常）からなる鍵関連情報を送信する。なお、移動局1と固定局2の鍵決定

のための通信②、⑤で、鍵関連情報を暗号化してもよい。

【0044】移動局1の鍵管理処理部5は、固定局2からの鍵関連情報によって自局のバージョンV1とその通常鍵K1の使用を確認する。次に、⑥移動局1は通信用DB4から平文の送信情報を暗号処理部7に読み込み、鍵情報DB6から読み出した使用鍵K1を用いて暗号化する。例えば、有料道路のETCシステムでは、料金引き落としのためのICカード番号や残金額などが暗号化されて送信される。そして、⑧通信処理部8から固定局2に暗号文を送信する。⑨固定局2の復号処理部9は、受信した暗号文を鍵情報DB13の識別子(N××1)に対応する鍵K1によって、平文に復号する。

【0045】これによれば、移動局の通信要求により固定局との間で使用鍵を決定する処理のみで、両者間の通信が即座に開始できるので、通信時間が約0.1秒以下に制限される有料道路のETCシステムにも適用可能である。また、暗号化/復号化に用いる使用鍵そのものは鍵関連情報に含まず、通信されないため、システムの高セキュリティを確保できる。

【0046】図8に、鍵緊急更新で使用鍵を決定する場合の移動局と固定局間の処理の流れを示す。移動局1の鍵管理処理部5は、①鍵情報DB6に有効管理されているバージョンV1を読み出し、②固定局2に送信要求メッセージと共に送信し、③固定局2の鍵管理制御処理部14がバージョンV1のサポートを確認するまでは、通常通信の場合と同様である。④確認の結果、バージョンV1の通常鍵K1が無効、緊急鍵K1'が有効の場合、バージョンV1の緊急鍵K1'を使用鍵に決定し当該移動局の識別子(N××1)と対応付けて鍵情報DB13へ登録し、⑤当該移動局へバージョンV1と鍵用途(緊急)からなる鍵関連情報を送信する。

【0047】移動局1の鍵管理処理部5は、⑥固定局2からの鍵用途によって自局の通常鍵K1の有効を知ると、鍵情報DB6の通常鍵K1の有効フラグを無効にする。暗号処理部7は平文の暗号化に際し、鍵情報DB6で有効に管理されているK1'を使用する。移動局1から固定局2への暗号文の送信(⑧)以降は、通常通信の場合と同様である。なお、移動局1から固定局2へ通信要求時の鍵関連情報に鍵バージョンと共に鍵用途を含めると、緊急鍵を使用している固定局側の鍵決定処理を簡単化できる。このとき、固定局2から移動局1へ応答する鍵関連情報は鍵バージョンのみでよい。

【0048】ところで、固定局における通常鍵の有効/無効の管理は、上位装置から特定の鍵バージョンに対する無効指示によって行なわれる。すなわち、移動局の利用料金などを清算する中央装置などで、一つの移動局に対して複数の固定局から物理的に不可能な同時の利用の事実を検出した場合や、ユーザからの苦情申立てがあった場合に、不正使用が発生したと判断して通常鍵の無効

を指示する。

【0049】図9に、固定局における通常鍵の無効化の処理フローを示す。鍵管理制御処理部14は、上述した通信鍵決定の処理機能(図6)の外に、通常鍵無効化の処理機能を有している。まず、上位装置からの鍵用途変更指示の受信を待つ(S301)。上位装置から、鍵バージョンを指定した鍵用途の変更指示を受信すると、指定されたバージョンの通常鍵を無効にし、鍵情報管理DB12の当該有効フラグを無効に設定する(S302)。なお、本処理は、鍵決定処理に対する割込みによって処理してもよい。

【0050】本実施例によれば、不正使用が発覚した鍵バージョンの通常鍵を無効にし、各移動局が保持している緊急鍵への切り替えをオンラインで処理できるので、不正使用による被害の拡大を防止しながらシステムの通常の運用を維持できる。また、緊急鍵のデータを互いに通信することなく切り替えるので、高セキュリティな対応が可能になる。

【0051】例えば、有料道路のETCシステムでは、通常の移動局のバージョン更新は定検時などとなるので、不正による被害の拡大によりシステム停止に追い込まれる恐れがある。しかし、本実施例によれば、緊急鍵への切り替えが通常利用の通信中にオンラインで自動処理されるので、システムにもユーザにも負担がなく使い勝手が良い。

【0052】以上の実施例では移動局と固定局の暗号通信の暗号鍵に対称鍵を用いたが、本発明の移動通信は暗号鍵に非対称鍵、または暗号アルゴリズムを変更するアルゴリズム鍵等によっても実現できる。

【0053】また、上述した対称鍵暗号方式では、移動局と固定局に予め通常鍵と緊急鍵からなる対称鍵を用意している。しかし、固定局は通常鍵のみをインストールしておき、上位装置から固定局への鍵用途変更指示に付加して当該バージョンの緊急鍵を送信するようにしてもよい。これにより、固定局での盗難等による緊急鍵の露見を防止できる。なお、上位装置からの鍵情報の通信による漏洩の危険が伴うので一時的な緊急対策とし、抜本的には移動局のバージョン更新が必要になる。

【0054】

【発明の効果】本発明の移動体通信方法によれば、固定局と複数の移動局とで共通鍵の複数のバージョンを共用する場合に、移動局の通信要求時のバージョンを確認して固定局自身で使用鍵を決定できるので、移動局との通信を速やかに開始できる。

【0055】また、対称鍵暗号方式を採用するので、不正使用が発覚した場合等に各移動局が保持している代替鍵への切り替えを、暗号鍵を送信することなくオンライン処理で実効できるので、不正使用の被害の拡大を防止できる。

【0056】本発明の移動体通信システムによれば鍵サ

ーバを不要とするので、システム構成が簡素化するとともに、高セキュリティを確保できる。また、緊急時の鍵切り換えを通信中に自動処理するので使い勝手がよい。

【図面の簡単な説明】

【図1】本発明の一実施例による移動体通信システムの構成図。

【図2】対称鍵暗号方式を用いた移動局の鍵情報DBのデータ構成図。

【図3】対称鍵暗号方式を用いた固定局の鍵管理情報DBのデータ構成図。

【図4】固定局の通話中の使用鍵を管理する鍵情報DBの構成図。

【図5】移動局の対称鍵暗号方式による使用鍵の決定処理を示すフロー図。

【図6】固定局の対称鍵暗号方式による使用鍵の決定処理を示すフロー図。

【図7】移動局と固定局間の通常の鍵決定の処理とデータの流れを示す説明図。

【図8】移動局と固定局間の鍵緊急更新の処理とデータ*

*の流れを示す説明図。

【図9】上位指示により、固定局の通常鍵無効化処理を示すフロー図。

【図10】有料道路の自動料金収受システム（ETC）の概略の構成図。

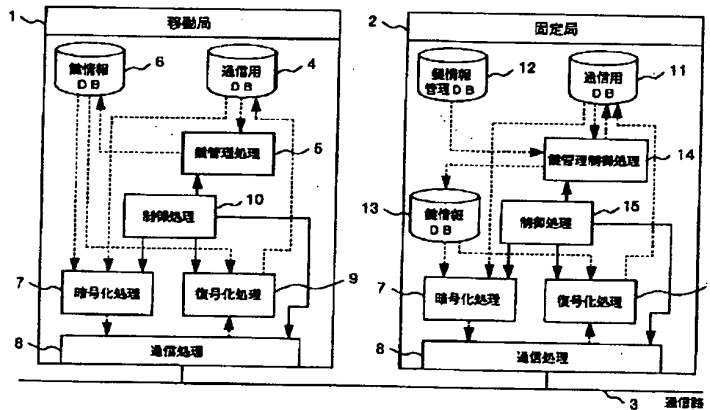
【図11】鍵サーバ問合せによる鍵決定動作を示す従来の移動体通信システムの説明図。

【符号の説明】

1…移動局、2…固定局、3…通信路、4…通信用DB、5…鍵管理処理部、6…鍵情報DB（移動局側）、7…暗号化処理部、8…通信処理部、9…復号化処理部、10…制御処理部（移動局側）、11…通信用DB、12…鍵情報管理DB、13…鍵情報DB（固定局側）、14…鍵管理制御処理部、15…制御処理部（固定局側）、21…鍵バージョン、22…鍵用途、23…対称鍵、24…有効フラグ、31…移動局識別子、32…使用鍵、100…固定局、110…アンテナ、200…専用レーン、210…通信エリア、300…車両、310…移動局。

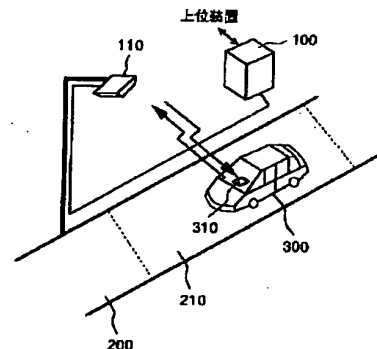
【図1】

図 1



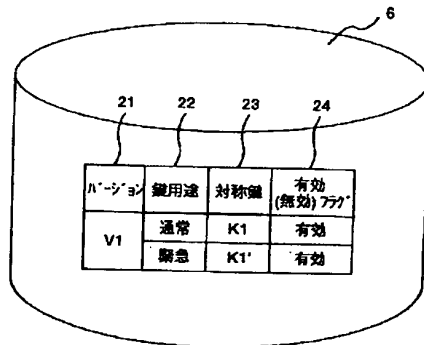
【図10】

図 10



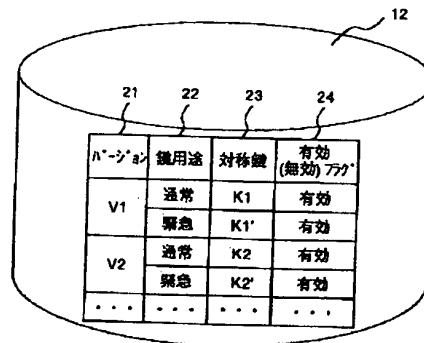
【図2】

図 2



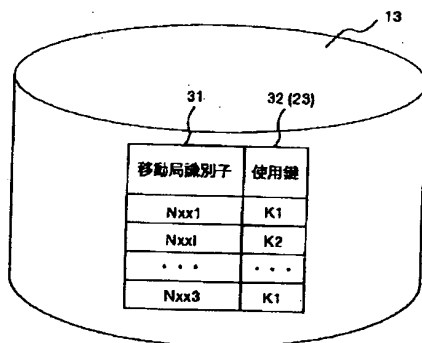
【図3】

図 3



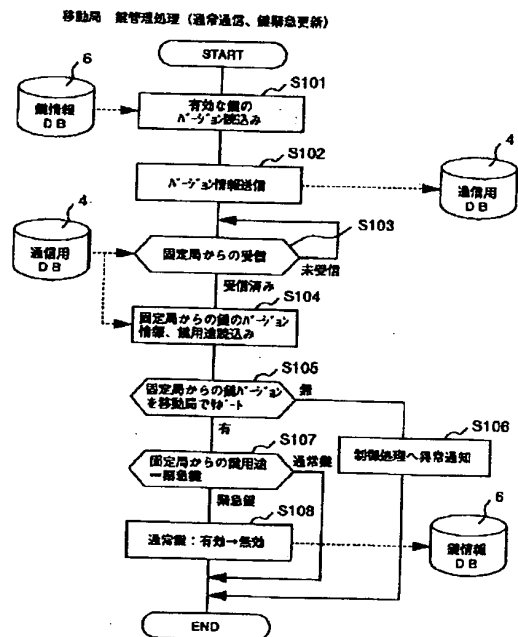
【図4】

図 4



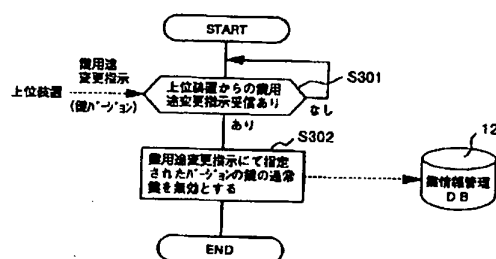
【図5】

図 5

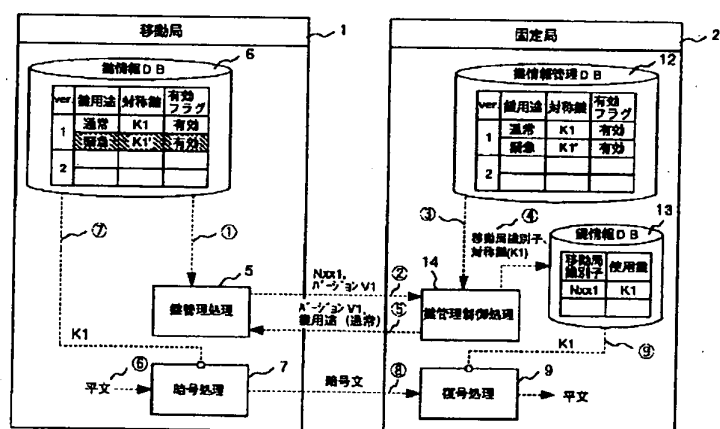


【图9】

9

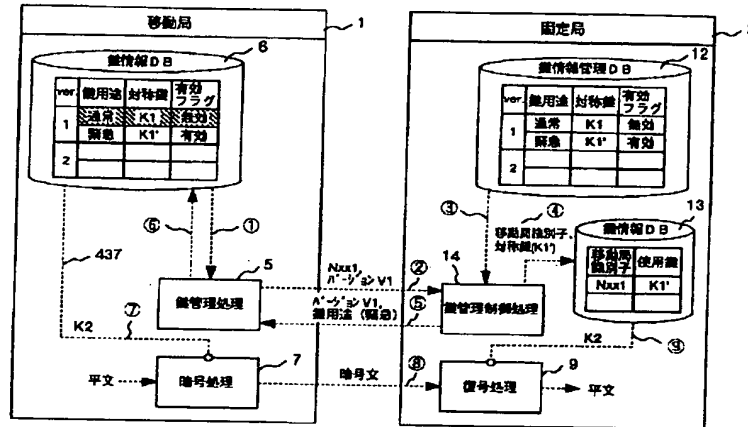


7



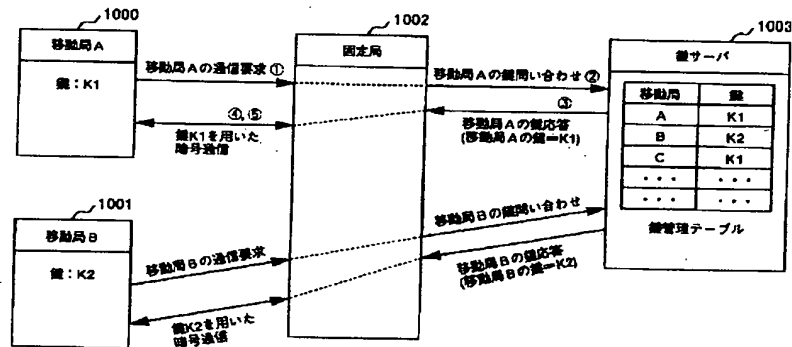
【図8】

図 8



【図11】

図 11



フロントページの続き

(51)Int.Cl.⁶

識別記号

F I

H 0 4 L 9/00

6 0 1 B

(72)発明者 飯野 隆之

茨城県日立市大みか町五丁目2番1号 株
式会社日立製作所大みか工場内

(72)発明者 織茂 昌之

神奈川県川崎市麻生区王禅寺1099番地 株
式会社日立製作所システム開発研究所内

(72)発明者 福澤 寧子

神奈川県川崎市麻生区王禅寺1099番地 株
式会社日立製作所システム開発研究所内

(72)発明者 石田 修一

神奈川県川崎市麻生区王禅寺1099番地 株
式会社日立製作所システム開発研究所内